Atty. Docket No.: LYRN002US0
Customer ID No. 58,293

In the Claims:

7. (Cancelled)

8. (Cancelled)

9. (Cancelled)

10. (Cancelled)

11. (Cancelled)

17.(Cancelled)

18. (Cancelled)

19. (Cancelled)

32.(New) A method of encrypting data, comprising:

choosing a modulus C for modular calculations, wherein the modulus C is selected from the group consisting of (a) w-big and w-heavy, and (b) w-little and w-light; and

using the modulus to encrypt data.

33. (New) The method of claim 32, further comprising:

performing a ring arithmetic function on numbers, including (a) using a residue number multiplication process, (b) converting to a first basis using a mixed radix system, and (c) converting to a second basis using a mixed radix system.

34. (New) The method of claim 32, wherein the modulus C is of the form 2^w - L, and wherein L is a low Hamming weight odd integer less than $2^{(w-1)/2}$.

35. (New) The method of claim 34, further comprising:

calculating the modulus C by a process including

(a) splitting P into 2 w-bit words H_1 and L_1;

(b) calculating $S_1 = L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + ... + (H_1 2^{xk}) \div H_1$;

(c) splitting S_1 into two w-bit words H_2 and L_2;

(d) computing $S_2 = L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + ... + (H_2 2^{xk}) + H_2$;

(e) computing $S_3 = S_2 + (2^{x1} + ... + 2^{xk} + 1)$;

(f) determining the modulus C by comparing S_3 to 2w, wherein the modulus C = S_2 if $S_2 < 2^w$, and wherein the modulus $C = S_3 - 2^w$ if $S_3 \geq 2^w$;

wherein the modulus C is a residue.

36. (New) The method of claim 32, wherein the modulus C is of the form $2^w + L$, and wherein the modulus C has a Hamming weight close to 1.

37. (New) The method of Claim 32, wherein the method of encrypting data comprises a method of cryptographic hashing.

38. (New) The method of Claim 32, wherein the modulus C is w-big and w-heavy.

39. (New) The method of Claim 32, wherein the modulus C is w-little and w-light.